

## Claims

1-2. (canceled)

3. (currently amended) A computer-readable medium containing instructions for performing ~~the method of claim 2~~ a method for transforming a message represented as an element of a complete residue set modulo a prime number  $p$  into a Montgomery residue of a multiplicative inverse, the method comprising:

selecting a Montgomery radix  $R = 2^m$ , wherein  $m$  is an integer multiple of a wordsize, and  $m$  is greater than a bit-length of the prime number  $p$ ;

determining  $(r, k)$  from an almost Montgomery inverse function;

if  $k$  is less than  $m$ , then assigning  $r$  a value obtained as a Montgomery product of  $r$  and  $R^2 \bmod p$ , and assigning  $k$  a value  $k = k + m$ ; and

obtaining the multiplicative inverse as a Montgomery product of  $r$  and  $2^{2m-k}$ ; and

retrieving a stored value of  $R^2 \bmod p$ .

4. (canceled)

5. (currently amended) A cryptographic system for encryption and decryption, the system comprising a module for transforming a message ~~as recited in claim 1~~ according to a method comprising:

representing the message as an element of a complete residue set modulo a prime number  $p$ ;

selecting a Montgomery radix  $R = 2^m$ , wherein  $m$  is an integer multiple of a wordsize, and  $m$  is greater than a bit-length of the prime number  $p$ ;

determining  $(r, k)$  from an almost Montgomery inverse function;

if  $k$  is less than  $m$ , then assigning  $r$  a value obtained as a Montgomery product of  $r$  and  $R^2 \bmod p$ , and assigning  $k$  a value  $k = k + m$ ;

obtaining the multiplicative inverse as a Montgomery product of  $r$  and  $2^{2m-k}$ ; and

representing the transformed message as a Montgomery residue of the multiplicative inverse..

6-7. (cancelled)

8. (currently amended) A cryptographic system, comprising an encryption/decryption module

that performs ~~the method of claim 7~~ a method for obtaining a classical inverse of a message,  
comprising:

assigning a series of binary digits to the message, wherein the assigned binary digits represent  
an element of a residue set modulo a prime number  $p$ ;

obtaining values  $(r,k)$  by calculating an almost Montgomery inverse function of the  
representation of the message using a Montgomery radix  $R = 2^m$ , wherein  $m$  is an integer multiple of a  
wordsize and is greater than a bit-length of the prime number  $p$ ;

if  $k$  is greater than  $m$ , then assigning  $r$  a value equal to a Montgomery product of  $r$  and 1, and  
assigning  $k$  a value of  $k - m$ ; and

calculating the classical inverse as a Montgomery product of  $r$  and  
 $2^{m-k}$ .

9. (previously presented) The cryptographic system of claim 8, further comprising at least one integrated circuit.

10. (currently amended) A computer-readable medium, comprising instructions for performing ~~the method of claim 7~~ a method for obtaining a classical inverse of a message, comprising:  
assigning a series of binary digits to the message, wherein the assigned binary digits represent  
an element of a residue set modulo a prime number  $p$ ;

obtaining values  $(r,k)$  by calculating an almost Montgomery inverse function of the  
representation of the message using a Montgomery radix  $R = 2^m$ , wherein  $m$  is an integer multiple of a  
wordsize and is greater than a bit-length of the prime number  $p$ ;

if  $k$  is greater than  $m$ , then assigning  $r$  a value equal to a Montgomery product of  $r$  and 1, and  
assigning  $k$  a value of  $k - m$ ; and

calculating the classical inverse as a Montgomery product of  $r$  and  
 $2^{m-k}$ .

11-18. (cancelled)

19. (currently amended) A computer-readable medium containing instructions for performing ~~the method of claim 16~~ a method for computing a multiplicative inverse of an  $M$ -residue  $A = a2^m \bmod p$ , wherein  $p$  is a prime number,  $m$  is an integer, and a Montgomery radix  $R = 2^m$ , the method

comprising:

computing an intermediate product  $r$  and an integer  $k$  using an almost Montgomery inverse procedure;

retrieving a value of  $R^2 \bmod p$ ;

assigning an intermediate product  $r'$  the value of a Montgomery product of  $r$  and  $R^2$ ; and

obtaining the multiplicative inverse as a Montgomery product of  $r'$  and  $2^{2m-k}$ .

20-21. (canceled)